UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/714,521	11/17/2003	Lionel Belnet	550-484	6841

23117 7590 12/10/2007

NIXON & VANDERHYE, PC
901 NORTH GLEBE ROAD, 11TH FLOOR
ARLINGTON, VA 22203

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
12/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/714,521	BELNET ET AL.	
	Examiner	Art Unit	
	Eleni A. Shiferaw	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 September 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

1. The applicant mentions that the UK search report is submitted with his/her response on 09/24/2007; however no document is attached with the response.

2. "Trusted Computing Group...," submitted with the information disclosure statement on 11/17/03 has been considered, on December 6, 2007.

Response to Arguments

3. Applicant's arguments filed 9/24/07 have been fully considered but they are not persuasive.

Regarding argument the reference failure to disclose secure and non-secure domains and modes, remark page 15 par. 2, argument is not persuasive because Letwin discloses a method of executing computer programs in a multi-mode microprocessor (see col. 1 lines 4-7). The multi-modes are protected mode and unprotected modes and/or real mode (see par. 1 lines 19-24). The secure and non-secure domains are described in fig. 1-3 of Letwin.

Regarding argument the reference failure to teach wherein "said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode", remark page 15 par. 3, argument is not persuasive because Letwin discloses a method of operating a multi-mode processor that will enable a mixture of programs designed to run in the various modes of the

microprocessor, i.e. during non-protected mode, secure programs/data are not accessible and/or access is interrupted (see col. 3 lines 35-col. 4 lines 58).

Regarding argument reference failure to disclose "a memory configured to store data required by the processor and comprising secure memory for storing secure data and non-secure memory for storing non-secure data.", remark page 15 par. 4, argument is not persuasive because Letwin discloses storing secure programs/data in protected mode and non secure program/data in unprotected mode so secure data can not be accessed when mode is unprotected (see col. 4 lines 17-36 and col. 7 lines 15-21).

Regarding argument the reference failure to disclose "a non-secure table and a secure table, the non-secure table being within the non-secure memory and ... the secure table being within the secure memory.", remark page 16 par. 1, argument is not persuasive because Letwin teaches "protected mode descriptor tables" are in protected mode and unprotected mode descriptor tables are described in Letwin (col. 4 lines 5-16, col. 9 lines 51-col. 10 lines 53, and fig. 3).

Regarding argument the reference failure to teach wherein "non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor.", page 16 par. 2, argument is not persuasive because Letwin teaches "protected mode descriptor tables" are in protected mode and unprotected mode descriptor tables are described in Letwin (col. 4 lines 5-16, col. 9 lines 51-col. 10 lines 53, and fig. 3), real mode

addressing (col. 10 lines 6-33), protected and unprotected mode addressing is also disclosed in Letwin (col. 10 lines 34-col. 11 lines 12).

Regarding argument the reference failure to teach "the internal storage unit comprising a flag associated with each descriptor stored within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table.", remark page 16 par. 3, argument is not persuasive because Letwin discloses an indicator or "flag" is included for each program that indicates whether the program is designed to run in real or protected mode (see col. 7 lines 6-27) ... to identify if the descriptor is from secure table, descriptor flags GDT, LDT, ... (col. 7 lines 6-27, fig. 3, and col. 11 lines 12-58).

Regarding argument failure to disclose wherein "the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table.", remark page 17 par. 2, argument is not persuasive because Segments contain program subroutines and segments are selected in multiple modes and/or LDT is not accessible during GDT (Letwin col. 10 line 6-col. 11 lines 58).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-3, 6-10, 12-15, 18-22, and 24 are rejected under 35 U.S.C. 102(b) as being anticipated by Letwin EP 0 574 032 A1.

Regarding claim 1, Letwin anticipates a data processing apparatus, comprising:

a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain (col. lines 19-24, and col. 6 lines 42-50), said processor being configured such that when executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode (col. 4 lines 17-36);

a memory configured to store data required by the processor (col. 7 lines 15-21) and comprising secure memory for storing secure data and non-secure memory for storing non-secure data (col. 4 lines 17-36, and col. 7 lines 15-21), the memory containing a non-secure table and a secure table (col. 4 lines 5-16 and fig. 3), the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor (col. 9 lines 51-col. 10 lines 53), and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor (col. 9 lines 51-col. 11 lines 12); and

a memory management unit configured, upon receipt of a memory access request issued by the processor when access to an item of data in the memory is required, to perform one or more predetermined access control functions to control issuance of the memory access request to

the memory, the memory management unit comprising an internal storage unit configured to store descriptors retrieved by the memory management unit from either the non-secure table or the secure table (col. 10 lines 6-53), and the internal storage unit comprising a flag associated with each descriptor stored (col. 7 lines 6-27) within the internal storage unit to identify whether that descriptor is from said non-secure table or said secure table (col. 7 lines 6-27, fig. 3, and col. 11 lines 12-58);

when the processor is operating in said at least one non-secure mode, the memory management unit being configured to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table (col. 10 lines 6-col. 11 lines 58), and when the processor is operating in said at least one secure mode, the memory management unit being configured to perform the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the secure table (col. 10 lines 6-col. 11 lines 58, and col. 20 lines 29-40).

Regarding claim 13, Letwin anticipates a method of managing access to a memory in a data processing apparatus, the data processing apparatus comprising a processor configured in a plurality of modes and a plurality of domains, said plurality of domains comprising a secure domain and a non-secure domain, said plurality of modes including at least one non-secure mode being a mode in the non-secure domain and at least one secure mode being a mode in the secure domain (col. lines 19-24, and col. 6 lines 42-50), said processor being configured such that when

executing a program in a secure mode said program has access to secure data which is not accessible when said processor is operating in a non-secure mode (col. 4 lines 17-36), the memory being configured to store data required by the processor (col. 7 lines 15-21) and comprising secure memory for storing secure data and non-secure memory for storing non-secure data, the memory containing a non-secure table and a secure table (col. 4 lines 17-36, and col. 7 lines 15-21), the non-secure table being within the non-secure memory and arranged to contain for each of a number of first memory regions an associated descriptor (col. 9 lines 51-col. 10 lines 53), and the secure table being within the secure memory and arranged to contain for each of a number of second memory regions an associated descriptor (col. 9 lines 51-col. 11 lines 12), the method comprising the steps of:

(i) issuing from the processor a memory access request when access to an item of data in the memory is required (col. 4 lines 2-16);

(ii) determining whether an internal storage of a memory management unit contains a required descriptor from which access control information can be derived to enable the memory management unit to perform one or more predetermined access control functions to control issuance of the memory access request to the memory (col. 4 lines 2-36);

(iii) in the event that the required descriptor is not contained within the internal storage unit, retrieving from either the non-secure table or the secure table, depending on the mode of operation of the processor, the required descriptor, storing that required descriptor within the internal storage unit, and setting a flag to be associated with that required descriptor within the internal storage unit to identify whether that required descriptor is from said non-secure table or said secure table (col. 7 lines 2-28, and col. 10 lines 6-53); and

(iv) using the access control information derived from the required descriptor to perform within the memory management unit one or more predetermined access control functions to control issuance of the memory access request to the memory (col. 4 lines 2-58); such that when the processor is operating in said at least one non-secure mode, the memory management unit performs the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the non-secure table (col. 10 lines 6-col. 11 lines 58), and when the processor is operating in said at least one secure mode, the memory management unit performs the predetermined access control functions for the memory access request with reference to access control information derived from the descriptors in the internal storage unit retrieved from the secure table (col. 10 lines 6-col. 11 lines 58, col. 20 lines 29-40 and fig. 3).

Regarding claims 2 and 14, Letwin further discloses a data processing apparatus/method, wherein in said at least one non-secure mode the processor is configured under the control of a non-secure operating system, and in said at least one secure mode the processor is configured under the control of a secure operating system, and wherein the descriptors in the non-secure table are generated by the non-secure operating system and the descriptors in the secure table are generated by the secure operating system (col. 10 lines 6-col. 11 lines 58).

Regarding claims 3 and 15, Letwin further discloses data processing apparatus/method, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each

descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region (fig. 3, fig. 10 lines 34-53, and fig. 4).

Regarding claims 6 and 18, Letwin discloses a data processing apparatus/method, wherein the non-secure table comprises a plurality of non-secure tables, each non-secure table containing descriptors pertaining to an associated process executable on the processor, the secure table comprises a plurality of secure tables, each secure table containing descriptors pertaining to an associated process executable on the processor, and the internal storage unit comprises an additional flag associated with each descriptor stored within the internal storage unit to identify the associated process to which that descriptor pertains (col. 10 lines 34-53 and col. 7 lines 6-20).

Regarding claims 7 and 19 data processing apparatus/method, wherein when the memory management unit needs to access the internal storage unit to derive access control information for use in performing the predetermined access control functions, the memory management unit determines from the flag and the additional flag for each descriptor in the internal storage unit whether the internal storage unit contains a descriptor that corresponds to the current mode of operation of the processor and the current process being executed on the processor (col. 7 lines 6-20).

Regarding claims 8 and 20 data processing apparatus, further comprising partition checking logic managed by the secure operating system, and configured whenever the memory access request is issued by the processor when operating in said non-secure mode to detect if the memory access

request is seeking to access the secure memory, and upon such detection to prevent the access specified by that memory access request (col. 20 lines 29-40).

Regarding claims 9 and 21 Letwin discloses a data processing apparatus/method, wherein the partition checking logic is configured, when the processor is operating in said at least one non-secure mode, to prevent the internal storage unit from storing access control information that would allow access to said secure memory (col.20 lines 27-58).

Regarding claims 10 and 22, Letwin discloses a data processing apparatus/method wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region (fig. 3, fig. 10 lines 34-53, and fig. 4), and wherein the partition checking logic is configured, when the processor is operating in said at least one non-secure mode, to prevent the internal storage unit from storing as access control information the physical address portion if the physical address that would then be produced for the virtual address is within the secure memory (col. 20 lines 27-58).

Regarding claims 12 and 24, Letwin further teaches a data processing apparatus/method, wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address

portion for the corresponding memory region (fig. 3, fig. 10 lines 34-53, and fig. 4), and wherein in the event that a descriptor within the non-secure table is associated with a memory region that at least partially incorporates a part of the secure memory, the partition checking logic is configured, when the processor is operating in non-secure mode, to prevent the internal storage unit from storing as access control information the physical address portion specified by that descriptor if the physical address that would then be produced for the virtual address is within the secure memory (col. 20 lines 27-58).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 4-5, 11, 16-17, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Letwin 0574032 A1 in view of Ellison et al. USPN 6,678,825 B1.

Regarding claims 4, 11, 23 and 16 Letwin discloses a data processing apparatus, wherein the internal storage unit comprises a main buffer configured to store the descriptors retrieved from the non-secure table or the secure table (fig. 3), and a buffer configured to store as access control information the physical address portions obtained from corresponding descriptors in the buffer for a number of corresponding virtual address portions, the memory management unit being configured to perform the conversion of the virtual address to the physical address with reference

to the content of the buffer (col. 10 lines 6-col. 11 lines 58); wherein the memory access request specifies a virtual address, and one of said predetermined access control functions comprises conversion of the virtual address to a physical address, each descriptor containing at least a virtual address portion and a corresponding physical address portion for the corresponding memory region (fig. 3, fig. 10 lines 34-53, and fig. 4), and wherein the partition checking logic is configured, when the processor is operating in said at least one non-secure mode, to prevent the transfer of a physical address portion from the main buffer to the buffer that would allow access to said secure memory (col. 11 lines 13-56). Letwin fails to explicitly disclose the translation buffers are translation lookaside buffer (TLB) and micro-TLB. However Ellison et al. discloses a translation buffers are translation lookaside buffer (TLB) and micro-TLB in a method of processor access control comprising a normal execution mode and isolated execution mode, and an access translation (see fig. 2A, col. 2 lines 65-col. 3 lines 9, col. 10 lines 50-col. 11 lines 19, and abstract). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings of Ellison within the system of Letwin because they are analogous in processor data access control. One would have been motivated to incorporate the teachings of Ellison because TLB buffer memory is well known at the time of the invention for processor data storage.

Regarding claims 5 and 17 the combination discloses a data processing apparatus/method, wherein the micro-TLB is flushed (fig. 1E and col. 6 lines 41-56) whenever the mode of operation of the processor changes between a secure mode and a non-secure mode, in the secure mode physical address portions only being transferred to the micro-TLB from a descriptor in the

main TLB that said associated flag indicates is from the secure table, and in the non-secure mode physical address portions only being transferred to the micro-TLB from a descriptor in the main TLB that said associated flag indicates is from the non-secure table (Letwin col. 10 lines 6-53, and Ellison see fig. 2A, col. 2 lines 65-col. 3 lines 9, col. 10 lines 50-col. 11 lines 19). The rational for combining are the same as claim 4 above.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

December 6, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100